أليكس هيرن | نشر في ١٧ أكتوبر ٢٠١٧,

خبراء أمنيون يحذرون من جميع شبكات "الواي فاي": احذر قد تعرضك للقرصنة

ترجمة حفصة جودة

اكتشف باحثون ضعفًا في شبكة الإنترنت اللاسلكية "الواي فاي"، حيث تمكنوا من كسر البروتوكول الأمني "WPA2" الذي يحمي أغلب شبكات الواي فاي، مما يشير إلى سهولة تعرض معظم شبكات الواي فاي إلى التنصت وهجمات القرصنة الخبيثة، كان ماثي فانهوف – خبير أمني في جامعة كيو ليوفين البلجيكية – قد اكتشف هذا الضعف في بروتوكول حماية الواي فاي ونشر تفاصيل هذا الخلل.

يقول فانهوف في تقريره: "يستطيع المهاجمون استخدام هذه التقنية الجديدة في الهجوم لقراءة المعلومات التي كان من المفترض تشفيرها بأمان، هذا الأمر قد يُستخدم في سرقة المعلومات الحساسة مثل أرقام بطاقة الائتمان وكلمات السر والرسائل والبريد الإلكتروني والصور وغيرهم.

أكد فانهوف أن الهجوم يعمل ضد جميع شبكات الواي فاي الحديثة، وبحسب إعدادات الشبكة فمن الممكن أيضًا إدخال بيانات أو التلاعب بالبيانات الموجودة، فعلى سبيل المثال يستطيع المهاجم حقن فيروس "رانسوموار" (فيروس يمنعك من دخول الحاسب قبل أن تدفع مبلغًا من المال) أو برامج ضارة أخرى على المواقع الإلكترونية، هذا الضعف يؤثر على العديد من أنظمة التشغيل والأجهزة مثل الأندرويد ولينكس وآبل وويندوز وأوبنبسد وميدياتك ولينكيس وغيرهم.

كتب فانهوف: "إذا كان جهازك يدعم الواي فاي فعلى الأغلب أنه تأثر بالضعف، فبشكل عام أي بيانات أو معلومات ينقلها الضحية يمكن فك تشفيرها، ووفقًا للجهاز المستخدم وإعدادات الشبكة فمن الممكن أيضًا فك تشفير البيانات المُرسلة إلى الضحية (مثل محتوى موقع على الإنترنت)"، منح فانهوف لهذا

الضعف اسمًا رمزيًا "كراك" (Krack، وهو اختصار لجملة "AttaCK Reinstallation Key" أي هجوم إعادة تثبيت الرموز).

من المفترض ألا يؤثر الهجوم على أمن المعلومات المرسلة من خلال شبكة محمية

قال مركز الأمن السيبراني الوطني البريطاني في بيان له إنه سوف يفحص هذا الضعف، وقال إنه حسب الأبحاث المنشورة عن الضعف العالمي لشبكات الواي فاي فيجب أن يكون المهاجم قريبًا بشكل مادي من الهدف وهذا الضعف المحتمل لن يضر بالتواصل بمواقع الإنترنت الآمنة مثل خدمات البنوك أو التسوق الإلكتروني.

أضاف مركز الأمن أنه يدرس البحث وسيقدم توجيهات إذا لزم الأمر، فأمن الإنترنت من أولويات المركز، كما أنهم يواصلون تحديث أجهزتهم في مواضيع مثل أمن الواي فاي وإدارة الأجهزة وأمن المتصفح، وكان فريق طوارئ الحاسبات الأمريكي "Cert" قد أطلق تحذيرًا عقب الحديث عن هذا الضعف.

يقول التحذير إن تأثير استغلال هذا الضعف يتضمن فك التشفير وقرصنة بروتوكول التحكم بالنقل وحقن محتوى "HTTP" وغيره، كما ذكر التحذير تفاصيل عدد الهجمات المحتملة وأضاف أن وجود الضعف في البروتوكول نفسه وليس في برنامج بعينه فجميع التطبيقات المطابقة للمعايير سوف تتأثر به.

من الضروري تطوير البروتوكول لأنه يستخدم بشكل عام في تشفير اتصالات الواي فاي، كانت المعايير الأمنية السابقة قد تعرضت للكسر، لكن البروتوكول الجديد كان متاحًا وقتها واستخدم على نطاق واسع.

الأهم من ذلك أنه من المفترض ألا يؤثر الهجوم على أمن المعلومات المرسلة من خلال شبكة محمية، هذا يعني أن الاتصال بمواقع الإنترنت المحمية ما زال آمنًا، من بين ذلك الاتصالات الأخرى المشفرة المستخدمة مثل "VPN" و"SSH".

الاتصال بمواقع الإنترنت غير المحمية لم يعد آمن

ومع ذلك، يجب أن نضع في اعتبارنا أن الاتصال بالمواقع التي لا تدعم صيغة "HTTPS" عامة وغير آمنة حتى يتم إصلاً هذا الضعف، وبالمثل، فمن الصعب تأمين اتصالات الإنترنت المنزلي بالكامل لفترة من الوقت، فأجهزة الاتصال اللاسلكي "الروتر" نادرًا ما يتم تحديثها، هذا يعني أنها ستستمر بالاتصال بطريقة غير آمنة، رغم ذلك يقول فانهوف إنه حتى لو تم تثبيت الإصلاح على الهاتف أو الحاسب فسيستمر الجهاز في الاتصال مع الروتر غير الآمن، هذا يعني أن مستخدمي أجهزة الروتر غير المحمية يجب أن يستمروا في إصلاح الأجهزة قدر الإمكان لضمان تأمين الشبكات الأخرى.

يقول أليكس هودسون – كبير الموظفين الفنيين- في شركة "Iron" إنه من الضروي التزام الهدوء، ويضيف: "التهديد الأمني عبر شبكة الواي فاي محدود لأنه يحتاج إلى القرب المادي، لذا فلن تجد فجأة أنك عرضة للهجوم من أي شخص على الإنترنت، لكن هذه الحماية ضعيفة ومن الضروري مراجعة مستوى تهديداتك".

بالإضافة إلى ذلك غالبًا ليس لدينا الكثير من البروتوكلات التي تعتمد على تأمين "WPA2" فقط، ففي كل مرة تستخدم بها موقعًا "HTTPS" فإن المتصفح الخاص بك يستخدم طبقات منفصلة من التشفير، لذا فدخول مواقع آمنة باستخدام الواي فاي ما زال أمرًا آمنا، ومن الجيد – رغم عدم وجود أي ضمان – أننا لا نحتاج لنقل الكثير من المعلومات باستخدام تشفير " WPA2 فقط.

الاعتماد على خاصية أمنية واحدة خطر للغاية

يقول كانديد ويست الباحث في شركة "سيمانتك" إن الهجوم على الشبكات بشكل كبير يحتاج لبعض الوقت، فهذه العملية معقدة نوعًا ما للقيام بها بسهولة، لكننا رأينا أشياء مشابهة لها ونعلم أنه من الممكن أن تصبح أوتوماتيكية، لذا يجب على أصحاب الشركات الصغيرة والناس في المنازل أن يأخذوا حذرهم نوعًا ما، وينصح ويست المستخدمين بتحديث برامجهم باستمرار.

أهم ما نستفيده من هذا الضعف كما يقول ويست هو أن الاعتماد على خاصية أمنية واحدة خطر للغاية، ويقول: "يجب ألا تثق في طريقة أمنية واحدة ولا تعتمد على تأمين الواي فاي فقط، استخدام " VPN أي وسيلة اتصالات آمنة أخرى أمر ضروري للغاية".

تتأثر الأجهزة وأنظمة التشغيل بشكل مختلف وفقًا لطريقة تشغيلها لبروتوكول "WPA2، أسوأهم وأكثرهم تضررًا نظام " Android 6.0 (Marshmallow) ونظام "Linux" نظرًا للكثير من الشوائب التي تجعل مفتاح التشفير يعيد كتابة جميع الأصفار، أما "iOS" و"Windows" فمن بين أكثر الأنظمة أمانًا في حالة عدم اعتمادهم بشكل كامل على بروتوكول "WPA2، ومع ذلك فجميع الأجهزة ليست محمية تمامًا من هذا الخلل.

قام فريق طوارئ الحاسبات الأمريكي "Cert" ومقره جامعة كارنيجي ميلون بإبلاغ شركات التكونولوجيا بهذا الخلل يوم 28 من أغسطس، هذا يعني أنه كان لديهم نحو شهر ونصف لإصلاح الخلل، وكانت صحيفة الغارديان قد تواصلت مع آبل وجوجل ومايكروسوفت ولينكسيس بشأن الموضوع، فقالت جوجل: "نحن على علم بالقضية وسنقوم بإصلاح الأجهزة المتأثرة خلال الأسابيع القادمة"، أما مايكروسوفت فقالت: "لقد أصدرنا تحديثًا أمنيًا لمعالجة المشكلة، وسيتم حماية جميع المستخدمين الذين حدثوا أجهزتهم"، أما بقية الشركات فلم يصل منهم أي رد.

المصدر: الغارديان